Claims

What is claimed is:

1. A method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation, the method comprising the steps of:

one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy}.

2. The method of claim 1, wherein the particular group, denoted as $G_{p,q}$, is a sub-group of a group Z_p^* where p and q are prime numbers such that p equals $rq + 1$ for a value r co-prime to q, and wherein the step of randomizing any portion of a result associated with the function that is outside the group $G_{p,q}$ is performed by computing a parameter h, randomly selected from the group Z_p^*, raising the parameter h to the exponent q and multiplying h^q by the result associated with the function.

3. The method of claim 1, wherein the one party is a client and the other party is a server.

4. The method of claim 1, further comprising the step of:

the one party receiving g^y from the other party and generating the shared secret g^{xy}.

5. The method of claim 4, further comprising the step of:

the one party authenticating the other party by comparing a received value against a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password.

6. The method of claim 4, further comprising the step of:

the one party transmitting a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password, to the other party whereby the other party may authenticate the one party.

7. The method of claim 4 further comprising the step of:

the one party generating a session key as a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password.

8. A method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation, the method comprising the steps of:

responsive to the one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, the other party performing the inverse group operation on m and the function of at least the password, removing the randomization of any portion of the result associated with the function that is outside the group, extracting g^x, and calculating the shared secret g^{xy}.

9. The method of claim 8, wherein the particular group, denoted as $G_{p,q}$, is a sub-group of a group Z_p^* where p and q are prime numbers such that p equals $rq + 1$ for a value r co-prime to q,

and wherein the step of randomizing any portion of a result associated with the function that is outside the group $G_{p,q}$ is performed by computing a parameter h, randomly selected from the group Z_p^*, raising the parameter h to the exponent q and multiplying h^q by the result associated with the function.

10. In accordance with a protocol for communication over a data network between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation, apparatus associated with the one party comprising:

at least one processor operative to: (i) generate a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized; and (ii) transmit m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy}.

11. The apparatus of claim 10, wherein the particular group, denoted as $G_{p,q}$, is a sub-group of a group Z_p^* where p and q are prime numbers such that p equals $rq + 1$ for a value r co-prime to q, and wherein the step of randomizing any portion of a result associated with the function that is outside the group $G_{p,q}$ is performed by computing a parameter h, randomly selected from the group Z_p^*, raising the parameter h to the exponent q and multiplying h^q by the result associated with the function.

12. The apparatus of claim 10, wherein the one party is a client and the other party is a server.

13. The apparatus of claim 10, wherein the at least one processor associated with the one party is further operative to receive g^y from the other party and generate the shared secret g^{xy}.

14. The apparatus of claim 13, wherein the at least one processor associated with the one party is further operative to authenticate the other party by comparing a received value against a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password.

15. The apparatus of claim 13, wherein the at least one processor associated with the one party is further operative to transmit a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password, to the other party whereby the other party may authenticate the one party.

16. The apparatus of claim 13, wherein the at least one processor associated with the one party is further operative to generate a session key as a function of at least one of an identifier of the one party, an identifier of the other party, m, g^y, the shared secret, and the password.

17. In accordance with a protocol for communication over a data network between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation, apparatus associated with the other party comprising:

at least one processor operative to, in response to the one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party: (i) perform the inverse group operation on m and the function of at least the

password; (ii) remove the randomization of any portion of the result associated with the function that is outside the group; (iii) extract g^x; and (iv) calculate the shared secret g^{xy}.

18. The apparatus of claim 17, wherein the particular group, denoted as $G_{p,q}$, is a sub-group of a group Z_p^* where p and q are prime numbers such that p equals $rq + 1$ for a value r co-prime to q, and wherein the step of randomizing any portion of a result associated with the function that is outside the group $G_{p,q}$ is performed by computing a parameter h, randomly selected from the group Z_p^*, raising the parameter h to the exponent q and multiplying h^q by the result associated with the function.

19. An article of manufacture for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation, the article comprising a machine readable medium containing one or more programs which when executed implement the steps of:

one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy}.

20. An article of manufacture for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an

inverse group operation, the article comprising a machine readable medium containing one or more programs which when executed implement the steps of:

responsive to the one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, the other party performing the inverse group operation on m and the function of at least the password, removing the randomization of any portion of the result associated with the function that is outside the group, extracting g^x, and calculating the shared secret g^{xy}.